Sub a1

We claim:

1. A communications network security method comprising:

identifying a plurality of routes that define the communications network;

identifying a plurality of hosts as a function of the plurality of routes;

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network;

probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address determined as a function of the topology; and

determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet.

2. The method of claim 1 wherein the source address is an IP address associated with a host external to the communications network and the packet is constructed as a function of the source address and an IP address associated with the at least one host.

3. The method of claim 2 wherein the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

4. The method of claim 2 wherein the performing the census operation further comprises:

pinging a plurality of IP addresses to verify their respective validity , the plurality of IP addresses being identified from the plurality of routes;

pinging particular hosts of the plurality of hosts to verify their respective location in the topology of the communications network;

performing at least a first DNS lookup for at least one of the particular hosts; and

performing at least a second DNS lookup across a communications channel, the communications channel serving to connect the communications network with a network

external to the communications network, the second DNS lookup identifying a specific host of the plurality of hosts.

5. The method of claim 3 wherein the probing the at least one host operation further comprises:

identifying the IP address associated with the probed host from the census; and

generating the packet as a function of the IP address associated with the probed host and the IP address associated with a host external to the communications network.

6. The method of claim 2 wherein the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk.

7. The method of claim 3 wherein the second packet is derived using at least a portion of information from the transmitted packet.

8. The method of claim 7 wherein the transmitted packet is a TCP packet.

9. The method of claim 8 wherein the second packet is a UDP packet or an ICMP packet.

10. A method for analyzing network security of a communications network, the method comprising:

identifying a plurality of routes that define the communications network;

identifying a plurality of hosts internal to the communications network as a function of the plurality of routes;

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network;

transmitting a packet from a host external to the communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet being generated as a function of an IP address associated with the host external to the communications network and an IP address associated with the particular one host of the plurality of hosts internal to the communications network; and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet.

11. The method of claim 10 wherein the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk.

12. The method of claim 11 wherein the second packet is derived using at least a portion of information from the transmitted packet.

13. The method of claim 12 wherein the performing the census operation further comprises:

pinging a plurality of IP addresses to verify their respective validity , the plurality of IP addresses being identified from the plurality of routes;

pinging particular hosts of the plurality of hosts to verify their respective location in the topology of the communications network;

performing at least a first DNS lookup for at least one of the particular hosts; and

performing at least a second DNS lookup across a communications channel, the communications channel serving to connect the communications network with a network external to the communications network, the second DNS lookup identifying a specific host of the plurality of hosts.

14. The method of claim 12 wherein the probed host is a dual-homed host.

15. The method of claim 11 wherein the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network.

16. A communications system comprising:

a first plurality of computers associated with a first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the plurality of computers, performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP address associated with a second computer of the second plurality of computers and an IP address associated with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet.

17. The communications system of claim 16 wherein the security host computer is associated with the first communications network.

18. The communications system of claim 17 wherein the response of the first computer the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

19. The communications system of claim 18 wherein the security host computer determines the security characteristic by monitoring the probed first computer to determine the response, and if the response includes a transmission of the second packet

from the probed host, generating a security alert message identifying the first computer as a security risk.

20. The communications system of claim 17 wherein the first communications network is an intranet and the second communications network is an Internet.

21. A security host computer comprising:

means for performing a census of a communications network and determining a topology of a first communications network, the topology being defined by at least one computer,

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of the topology, an IP address associated with a particular host computer associated with a second communications network and an IP address associated with the computer, the second communications network being separate from the first communications network; and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet.

22. The security host computer of claim 21 wherein the monitor monitors the computer to determine the response, and if the response includes a transmission of a second packet from the computer, a security alert message identifying the computer as a security risk is generated.

23. The security host computer of claim 22 wherein the security level is determined with respect to a firewall located between the first communications network and the second communications network.

24. A machine-readable medium having stored thereon a plurality of instructions, the plurality of instructions including instructions that, when executed by a machine,

cause the machine to perform of a method for identifying a plurality of routes that define the communications network; identifying a plurality of hosts as a function of the plurality of routes; performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network; probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet being derived as a function of the topology of the communications network; and determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet.

25. The machine-readable medium of claim 24 further comprising instructions that, when executed by a machine, cause the machine to perform the probing the at least one host operation by identifying the IP address associated with the probed host from the census; and generating the packet as a function of the IP address associated with the probed host and the IP address associated with a host external to the communications network.

26. The machine-readable medium of claim 25 wherein the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet.

27. The machine-readable medium of claim 26 wherein the communications network is an intranet, and the external host is associated with an Internet.